COMMONWEALTH OF MASSACHUSETTS

BARNSTABLE, ss.

SUPERIOR COURT
CRIMINAL ACTION
NO. 2072CR00046

COMMONWEALTH

vs.

JONATHAN T. FLEISCHMANN

MEMORANDUM OF DECISION AND ORDER ON DEFENDANT'S MOTION TO SUPPRESS SEARCH WARRANT

A grand jury indicted the defendant, Jonathan Fleischmann, of the following: home invasion, pursuant to G. L. c. 265, § 18C; kidnapping while armed with a firearm pursuant to G. L. c. 265, § 26; assault in a dwelling while armed with a firearm pursuant to G. L. c. 265, § 18A; assault to rape, pursuant to G. L. c. 265, § 24; assault with a dangerous weapon, pursuant to G. L. c. 265, § 15B(b); and assault and battery pursuant to G. L. c. 265, § 13A(a). The defendant moves to suppress all evidence obtained by the police as the result of the execution of a "geofence warrant," including the identification of the defendant, the subsequent search of his home and vehicle, statements made by the defendant, searches of phones owned by the defendant, and a search of the defendant's Google account. He argues that the warrant at issue constituted an impermissible "general warrant" in that it was overboard and lacking particularity and probable cause.[1] A hearing was held April 29, 2021 and the court took the matter under advisement. For the reasons that follow, the motion is **ALLOWED** in part and **DENIED** in part.

[1] A second warrant, which is not subject to the motion to suppress, was issued April 9, 2020.

BACKGROUND

The facts derive from the Application for Search Warrant ("Warrant Application"), the accompanying affidavit, and the record before the court on the Motion to Suppress.

On February 6, 2020, officers of the Yarmouth Police Department ("YPD") were dispatched to 7 Black Duck Lane to investigate a home invasion. The suspect was described by the alleged victims as a white male, approximately six-foot, one-inch to six-foot, two-inches tall, very thin, and wearing a black sweatshirt, black sweatpants, white sneakers with a red Nike "swoosh" and "jump man logo," and a black ski mask. He approached a sixteen-year-old girl, Danielle,[2] as she walked home from her school bus stop. The suspect told Danielle that he was from the electric company and asked if her parents were home. She responded that they were not, and he informed her that the power would be shut off over the next two days. He then appeared to leave by walking down the driveway. As she entered the passcode to her alarm system, the suspect, holding a gun, came up from behind her and attempted to force her into the home.

Another sixteen-year-old, Benjamin, who shared the same bus stop as Danielle, saw the man and the altercation. He ran toward the struggle, which caused the suspect to flee. The suspect left the property by way of the driveway and ran down Black Duck Lane toward Finch Lane. Then Benjamin chased the suspect until the suspect brandished the gun in his direction. Benjamin described the gun as black and similar in size to a "Glock."[3]

From a nearby house, YPD officers obtained surveillance footage, which showed a person, matching the suspect's description, running down Black Duck Lane and turning onto

[2] Because both alleged victims are minors and the indictments include a sexual offense, the court uses pseudonyms.
[3] It would be reasonable to infer that Benjamin's reference to a "Glock" was describing to the gun as a handgun.

Finch Lane at approximately 2:25 p.m. The individual appeared to be holding a black ski mask in his left hand, and his right hand appeared to hold a heavy object in his front, sweatshirt pocket.

A resident of Black Duck Lane stated that they saw also a man matching the suspect's description on Black Duck Lane at approximately 1:40 p.m. on the day of the incident. The resident stated that they had seen the individual walking east on Black Duck Lane, and several minutes later, walking west on Black Duck Lane. The individual walked down a neighbor's driveway and looked into the windows.

The Warrant

On February 9, 2020, Detective Eric Nuss ("Det. Nuss") of the Yarmouth Police Department applied for and was granted a type of search warrant colloquially known as a "geofence warrant." Such a warrant casts a virtual net around a specific location for a particular time frame in hopes of identifying a suspect under the theory that at least one of the identified devices might be associated with the individual.

Attachment A to the Warrant Application described a two-step process. First, it requested a warrant to retrieve data from Google, LLC, regarding cell site location information for individuals located within the vicinity of the incident on February 6, 2020, between 1:25 p.m. and 3:25 p.m. This time frame represents one hour prior to witness accounts of seeing the suspect and one hour after. The warrant requested data from all devices for two geofence locations: (1) a radius of fifty meters around Latitude: 41.663288, Longitude: -70.211556 or the immediate area around 7 Black Duck Lane in West Yarmouth; and (2) a radius of one hundred meters around Latitude: 41.662254, Longitude: -70.212651 or the immediate area around Merganser Lane, West Yarmouth. Google, LLC, would then provide the data anonymously,

meaning it would only provide an anonymized list of unique device tags for each of the devices captured within the two geofences.

Once YPD received the information related to the first step, the warrant permitted YPD to determine which device tags were relevant given their movement and locations. If additional location information for a given device tag was necessary to determine its relevance, the warrant authorized YPD to unilaterally request Google, LLC, to provide additional, undefined, location coordinates for the time period. For those device tags that YPD deemed relevant, Google, LLC, was required to provide to YPD, on demand, the subscriber information identifying the account holders or users of those devices, and provide "all information provided by the subscriber to the service provider to establish or maintain an account or communications channel," including the user's name, street address, telephone number, email addresses, the services subscribed to, six months of internet protocol ("IP") history, Short Message Service ("SMS") account number, and registration IP.

In the affidavit in support of the warrant, Det. Nuss opined that, in his training and experience, individuals involved in armed assaults and home invasions often communicate with co-conspirators through the use of cellular telephones, which have the ability to pinpoint an individual's location at a certain date and time. He knew ninety-six percent of American adults possess a cellular phone, the substantial majority of which possess a "smart" phone capable of internet use and mobile applications. He opined that such information "may reveal [a user's] presence in the area and ultimately lead to a successful identification of possible suspects in this investigation."

Further, Det. Nuss opined that he knew Google, LLC, collects and retains location data on their serves from Android-enabled mobile devices, which is a cellular phone using Google,

LLC's operating system, as well as devices on other operating systems, such as Apple iPhone, that support Google applications such as Google Search, Gmail, Google Maps, and Google Drive. This information is stored forever, unless deleted by the user. The detective noted that the specific parameters of when the data is collected is not entirely clear; Google, LLC, appears to collect the data not only when one of their services is activated and/or whenever there is an event on the device (such as a phone call, text message, internet access, or email access), but also when the user is not interacting with the device, such as when an application is simply "running in the background."

The warrant issued on February 19, 2020, and officers executed it on March 6, 2020. The warrant return yielded a list of anonymous Google Device ID's and the locations of those devices pursuant to the two geofences. YPD determined that only a single device traversed the two areas; they then requested and received the Google subscriber information associated with that Device ID. This data included a Google account ID number, the name associated with the account, "Tiff Miranda," the email address "jontiff2015@hotmail.com," and a recovery SMS phone number of 774-368-0443. It does not appear the remaining requested information was provided by Google, LLC, such as six months of historical IP information.

Second Search Warrant[4]

Det. Nuss applied for and was granted a second search warrant on April 9, 2020. The warrant sought, from Google, LLC, all data associated with the Device ID and email address noted above.

[4] Although the defendant does not seek suppression on the basis of the second warrant, the court includes a brief recitation of the facts regarding the second Warrant Application and accompanying affidavit in so much as is necessary to address the evidence the defendant has requested to be suppressed.

The accompanying affidavit, although similar to the initial search warrant application contained the more detailed, relevant information noted below.

In her interview with police after the incident, Danielle indicated that, in the months prior, she had seen a red "beat up" four-door car with a headlight out. She had seen it several times. On December 20, 2019, as Danielle walked home from her bus stop, she saw the vehicle make an aggressive three-point turn and drive by her in a slow manner. She then observed the vehicle make several more trips by her house as if it was "circling the neighborhood."

In the earlier-described surveillance footage, a red, four-door Pontiac sedan drove down Black Duck lane shortly before the incident. When the suspect ran in the footage, he ran in the direction that the sedan had driven.

On February 7, 2020, the affiant observed a red Pontiac traveling on Route 28 in the area of the incident. Det. Nuss queried the plate number, which returned the registered owner to be "August Miranda." Further investigation revealed that the vehicle had been stopped for a defective headlight and that, between September 3, 2019 and February 6, 2020, the vehicle had been stopped seven times. During each of those stops, the defendant was the operator.

Additional information, provided by an officer familiar with the defendant, indicated that the defendant resided in an apartment on Winslow Grey Road with his girlfriend, Tiffany Miranda. Det. Nuss estimated the apartment to be located approximately one block from the incident on Black Duck Lane. He also noted that the defendant was a level three sex offender and currently on probation. From prior investigations, Det. Nuss determined that the defendant was associated with a Cricket Wireless cellular phone number 774-368-0443. A subpoena was submitted to AT&T, the parent company of Cricket Wireless, for the phone records associated with the defendant's cellular phone.

On February 16, 2020, Danielle viewed over one thousand photographs at the YPD station and selected eighteen that "looked similar" to the defendant. Of the eighteen, she eliminated nine and highlighted a photograph of the defendant. She stated, "This guy could really be the guy."

On February 28, 2020, Benjamin participated in a photo array at the YPD station. He ultimately selected and initialed two photos that looked similar to the perpetrator. One of the two photos was a photo of the defendant.

On March 9, 2020, YPD obtained a warrant to arrest the defendant and search his home.[5] The YPD recovered, among other things, black sweatpants, a Cricket Wireless cellular phone which rang when officers dialed the defendant's known cellular phone number, and Reebok sneakers with a red pattern on the side. When officers turned the cellular phone on to put it in "airplane mode," a dark website and nude photo of a prepubescent female child came up on the screen. After the warrant was executed, police interviewed the defendant, who asked to speak with his girlfriend before talking with police. During the conversation with his girlfriend, he made incriminating statements, providing details of the 7 Duck Lane incident that were not released to the public.

ANALYSIS

A. The Defendant Has Standing to Challenge the Warrant

The Commonwealth argues that the defendant lacked standing to challenge the search of other Google users' data. However, suppression is appropriate where the evidence is obtained as a result of tainted cell site location information ("CSLI"). *Commonwealth* v. *Estabrook*, 472 Mass. 852, 864 (2015) (co-defendant's statements required suppression where he was confronted

[5] The court has not been provided with a copy of the Warrant Application, affidavit, or return for this warrant.

with defendant's tainted CSLI). Therefore, evidence obtained as a result of an improper "general" warrant may be challenged by the defendant.

B. The Information Sought Required a Warrant

The Commonwealth argues that the data requested falls under the six-hour "safe harbor rule" that applies to telephone call location data as established in *Commonwealth* v. *Augustine,* 467 Mass. 230, (2014) and *Commonwealth* v. *Estabrook,* 472 Mass. 852 (2015). It reasons that the data requested is akin to telephone call location data, as opposed to registration location data, in that Google, LLC only records the user's location when he or she elects to have a Google, LLC, application on his or her cellular phone. As such, it argues, the data is more akin to telephone call location data, which only records a phone's location when the user makes or receives a phone call. Furthermore, the Commonwealth contends that the "third party doctrine" applies and therefore the defendant has no legitimate expectation of privacy in the data.[6]

Generally, CSLI maintained by cellular services providers is subject to the warrant requirement as the privacy interest in one's movements, discoverable through the CSLI, is an interest that modern society recognizes as reasonable. *Carpenter* v. *United States*, 138 S. Ct. 2206, 2213 (2018). However, as discussed in *Commonwealth* v. *Augustine* and *Commonwealth* v. *Estabrook,* a defendant may not have an expectation of privacy in a shortened window of historical telephone call CSLI data. *Estabrook*, 472 Mass. at 858-859. See *Carpenter*, 138 S. Ct. at 2217 n.3 (there may be a limited period for which government may obtain CSLI free from Fourth Amendment scrutiny). The exception to the warrant requirement applies only to telephone call CSLI. See *Estabrook*, 472 Mass. at 858 n.12. Telephone call CSLI indicates the

[6] Pursuant to the "third party doctrine," courts have held that individuals lack a reasonable expectation of privacy in information they have revealed to a third party. See e.g. *Commonwealth* v. *Gosselin*, 486 Mass. 256, 263-264 (2020), and cases cited.

approximate physical location of cellular phone only when a telephone call is made or received, while registration CSLI provides approximate physical location every seven seconds unless powered off. *Id.*

In this case, the Warrant Application sought data stored by Google, LLC, as a result of either the phone being an Android phone, or as a result of the user having downloaded a Google application to their smart device. Pursuant to the affidavit, this data is collected continually, regardless of whether a user is actively making or receiving a phone call, as long as a Google-related application exists on their cellular phone. The affiant specifically noted that "almost all cellular phones and connected devices are either supported by Google or support Google software . . ." In addition, as part of step two, YPD sought "all information provided by the subscriber to the service provider to establish or maintain an account or communications channel," including the identifying information along with the services subscribed to and six months of IP history without additional judicial oversight. The affidavit acknowledged that such additional files are likely to contain location information digitally integrated into images, videos, or other files sent via the cellular phone to indicate the geographic location of the account user at a particular time.

The nature of the data requested, therefore, is more akin to registration data in that the user has little control, beyond an initial user agreement, to prevent his or her location from being transmitted, and may have nearly no control if they have an Android device. See *Carpenter* v. *United States*, 138 S. Ct. 2206, 2217 (2018) (noting all-encompassing record of holder's whereabouts); *Estabrook*, 472 Mass. 858 n.12; see also *State* v. *Pierce*, 222 A.3d 582, 585 (2019) (Android phone using Google operating system continually collects and sends Google data every ten to twenty minutes). Furthermore, the request for six months of IP history, which

can be used to determine an individual's location, is beyond the six hour "safe harbor" rule. *Estabrook*, 472 Mass. at 858. Therefore, the court considers this information as subject to the warrant requirement.

The Commonwealth's contention that the third party doctrine applies is similarly unavailing. *Carpenter* rejected the notion that CSLI data was subject to the third party doctrine, noting the "all-encompassing" nature of the data collected. See *Carpenter* v. *United States*, 138 S. Ct. 2206, 2217-2220 (2018) (government's retrieval of seven days of CSLI from third-party service provider qualified as search under the Fourth Amendment, notwithstanding third party doctrine). The Commonwealth's argument that the data here was not all-encompassing is belied by the information requested in the Warrant Application, which included the services to which the user subscribed and six months of IP history. See *Commonwealth* v. *Gosselin*, 486 Mass. at 263 (in distinguishing between medical and CSLI records in application of the third party doctrine, court noted government cannot use medical records to rummage through complex digital trains and location records created merely by participating in modern society). Although the *Carpenter*, *Estabrook*, and *Augustine* decisions noted that a search of shortened time periods of data may not carry the same Fourth Amendment implications, as noted above, the warrant authorized retrieval of six months of IP history, which the affidavit acknowledges can be used to determine location data. As such, the third party doctrine does not relieve the Commonwealth of the warrant requirement in this case.

C. The Warrant Was Overbroad

Having established that the data requested was subject to the warrant requirement, the court next determines whether the warrant was overbroad or sufficiently particularized. The Fourth Amendment to the United States Constitution, Article 14 of the Massachusetts

Declaration of Rights, and G. L. c. 276, § 2, require that a search warrant describe with particularity the places to be searched and the items to be seized. By defining and limiting the scope of the search, these constitutional and statutory particularity requirements prohibit general searches, and with regard to what is to be taken, nothing is left to the discretion of the officer executing the warrant. *Commonwealth* v. *Perkins*, 478 Mass. 97, 106 (2017) (additional citations and quotation omitted); *Commonwealth* v. *Wojcik*, 358 Mass. 623, 625 (1971).

The Warrant Application was written in such a manner that the initial inquiry appeared narrowly tailored; the warrant was curtailed to a two hour window, with an arguably specific radius to the scene of the crime.[7] However, the initial inquiry of step one was not the limit of what the warrant authorized. Rather, it authorized step one as well as step two without additional judicial oversight. Step two, as discussed, authorized officers of the YPD to exercise their own discretion in requesting additional location data outside the radiuses originally described as well as all user information known by Google, LLC, including six months of IP history, associated with any or all of the devices.

The Commonwealth highlights that, as a result of the initial inquiry, YPD was not provided a list of names, but rather only a list of device-identifying information. Only after the data was analyzed by YPD was the identifying information supplied for the defendant's device, which it argues could have been obtained via an administrative subpoena. This argument, however, focuses on the result of the search warrant as opposed to what the warrant authorized; although only an anonymous list was originally provided, the warrant authorized YPD to request the identifying information for *any* device on the list as well as additional location data, had the

[7] Although the Commonwealth submitted a map of both search radiuses, the maps are illegible. The relevance of 7 Black Duck Lane is apparent from the affidavit, however, there is no similar mention of Merganser nor any explanation as to why a radius of one hundred meters is required around this particular location, as opposed to the fifty meter radius around 7 Black Duck Lane.

YPD deemed it necessary or relevant without judicial oversight. This unbridled authority made the warrant impermissibly overbroad.[8]

D. Suppression

Although the court finds that the search warrant was overbroad, only the "fruits of the poisonous tree" must be suppressed. See *Commonwealth* v. *Wilson*, 486 Mass. 328, 336 (2020) (CSLI need not be suppressed if later search warrant satisfies independent source doctrine). As noted above, the defendant has requested suppression of all evidence obtained from the warrant, "including but not limited to the identification of the defendant, search of the defendant's home and car, statements made by the defendant, searches of phones owned by the defendant, and a search of the defendant's Google account."

The court agrees that fruit of the poisonous tree would include information related to the defendant's device as returned in the first warrant, and any statements made by the defendant as a result of the tainted CSLI data. However, the identification of the defendant appears to have been made independently of the warrant return; indeed, the defendant was identified by both alleged victims in photographs as potentially the perpetrator, he was routinely the driver of a vehicle matching the description of a suspicious vehicle, and lived nearby. See *Estabrook*, 472 Mass. at 865 (evidence initially discovered as consequence of unlawful search may be admissible if independently acquired by lawful means untainted by illegality).

[8] Because the warrant was overbroad, the court does not reach the issue of probable cause. However, in so much as the defendant emphasizes that the Commonwealth was unable to name the defendant as the intended target of the warrant, the court notes that simply because the Commonwealth does not name the defendant does not mean the warrant automatically lacks probable cause. See *Commonwealth* v. *Molina*, 476 Mass 388, 395 (2017). *Commonwealth* v. *Brown*, 68 Mass. App. Ct. 261 (2007) is not in conflict with this position as it determined that, only the search of the defendant's person pursuant to an "any persons present" warrant lacked probable cause.

In addition, the court has been provided with an insufficient record to determine whether suppression of the search of the defendant's home and vehicle is required. The defendant's identity and residential address appear to have been obtained by YPD prior to the execution of the illegal search warrant. However, whether that warrant properly articulated probable cause to search the defendant's residence and car cannot be determined on the record before the court. See *Id.* at 866 (court must determine whether sufficient facts in affidavit traceable to sources independent of illegally obtained CSLI to determine if suppression appropriate).

Turning to the issue of statements made by the defendant, the court agrees that statements made as a result of the tainted CSLI must be suppressed. However, the defendant requests a blanket suppression of all statements. Assuming that the defendant is specifically referring to the particularly incriminating statements that he made to his girlfriend while at the police station, the court cannot conclude on the record before it whether those statements were made as a result of the tainted CSLI data, or the result of a subsequent, potentially legal, warrant. *Id.*

Likewise, the legality of a search of the defendant's Google account, presumably pursuant to the second, unchallenged warrant, is not before the court. *Id.* However, as noted above, the information obtained from the initial, illegal warrant, must be suppressed.

ORDER

For the foregoing reasons, it is hereby **ORDERED** that the defendant's Motion to Suppress Search Warrant be **ALLOWED** in part and **DENIED** in part.

August 31, 2021

Mark C. Gildea
Justice of the Superior Court